Op afstand upgraden van Embedded Software

Gerard Fianen
INDES-IDS BV

Wie zijn wij ?

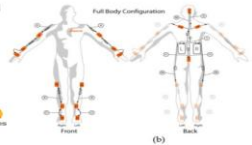
indes
The choice of professionals

Tools, software components and services for the development, testing and production of Real-Time Embedded Software










INDES -

Integrated Development Solutions BV

Wie zijn wij ?

indes
The choice of professionals

Tools, software components and services for the development, testing and production of Real-Time Embedded Software

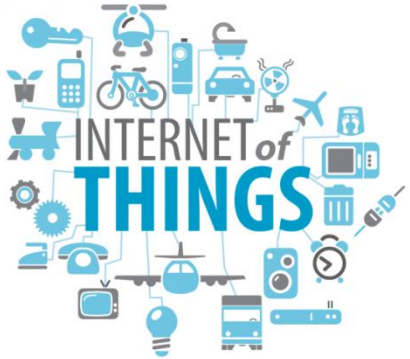
IAR SYSTEMS
SEGGER
SCIOPTA
i SYSTEM
ITTIA
percepio
SENSING SOFTWARE
freeRTOS
Sifos® Technologies

INDES -
Integrated Development Solutions BV

Remote Update / upgrade

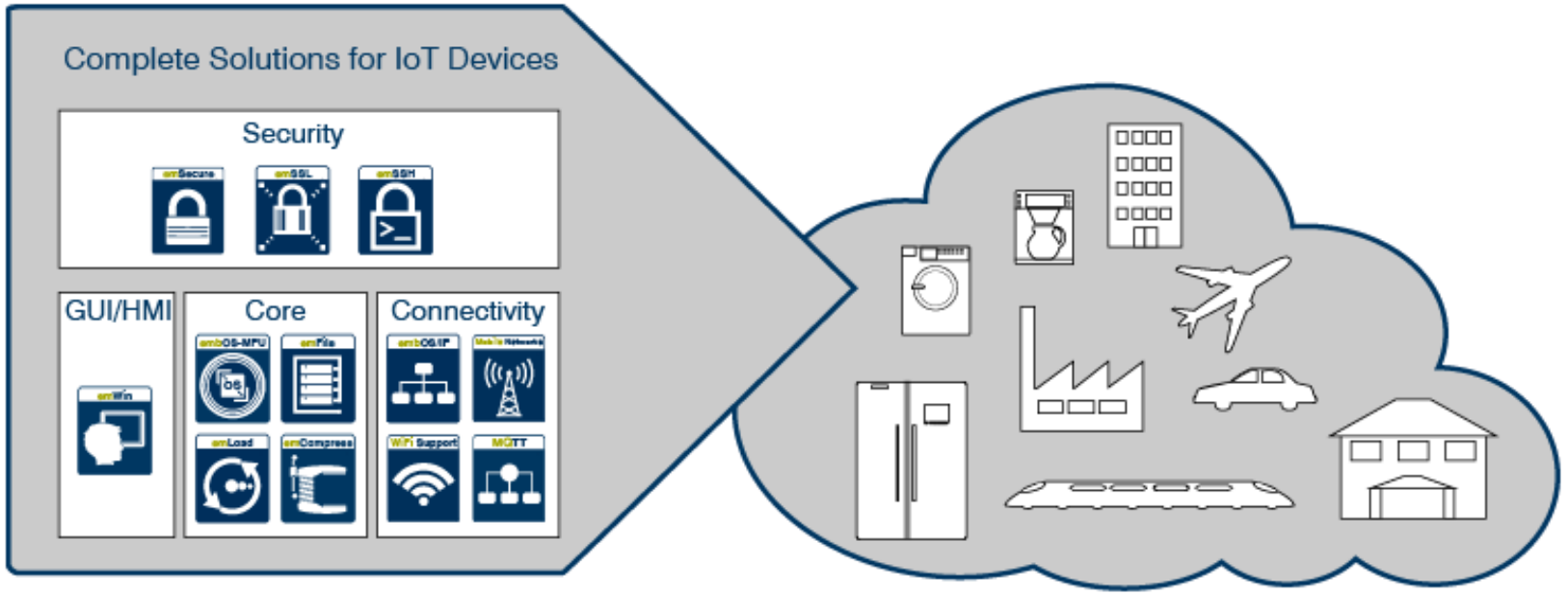
No access possible

Feature upgrades
Patches (i.pv. Recalls)
Feedback voor ADAS

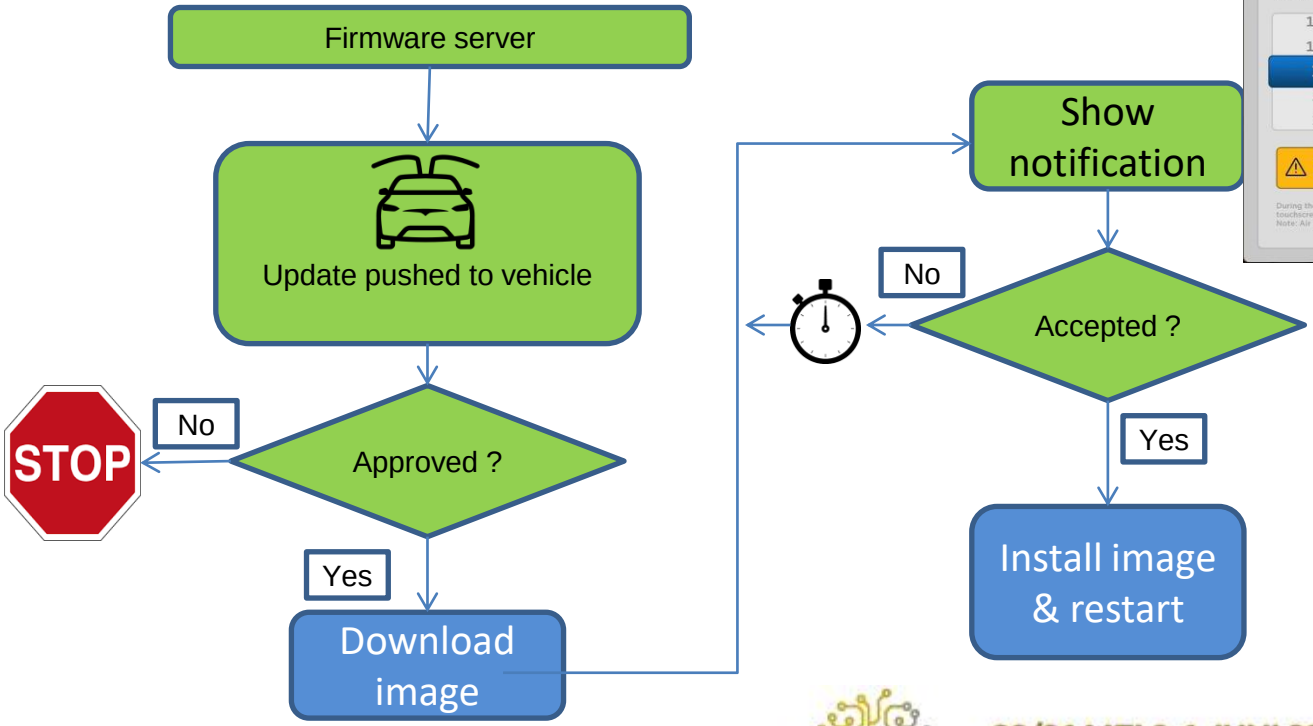


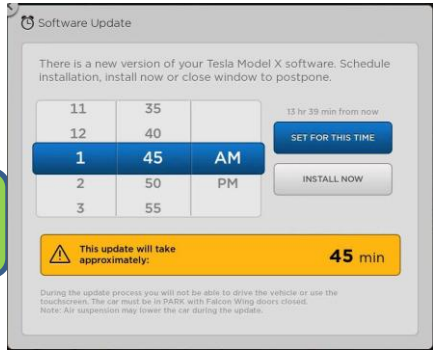
Security leak TLS / SSL
- Heartbleed
- Poodle

Components



Components -> solution





Important considerations

Security

- Communication
- Authentication

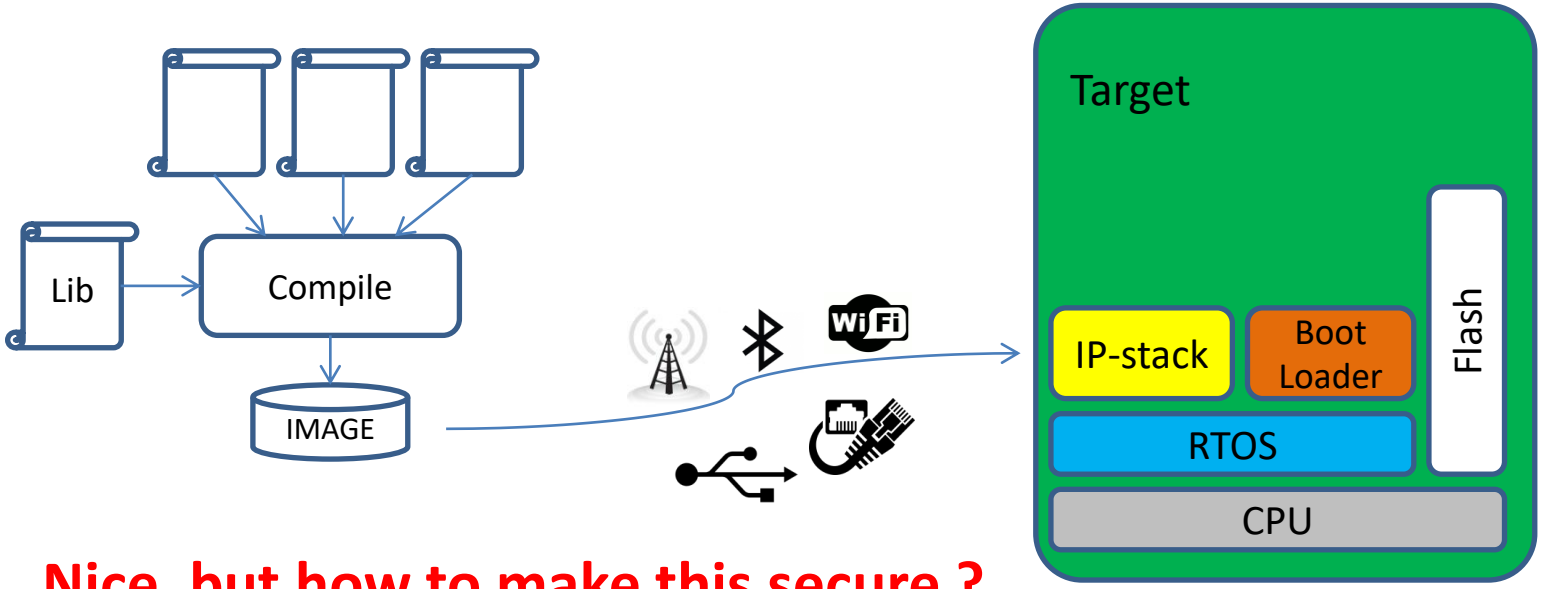
Constraints

-Bandwidth

-image code size

Transfer channel

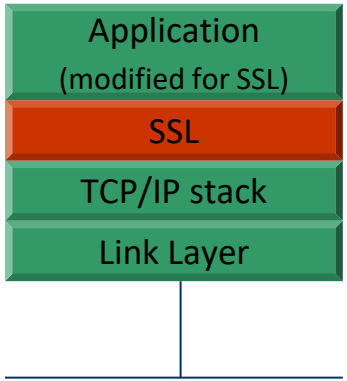
Bootloader



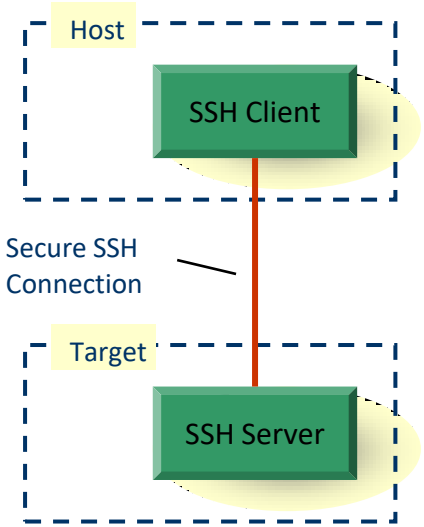
Nice, but how to make this secure ?

Secure communication

- Secure Socket Layer
- Secure Shell



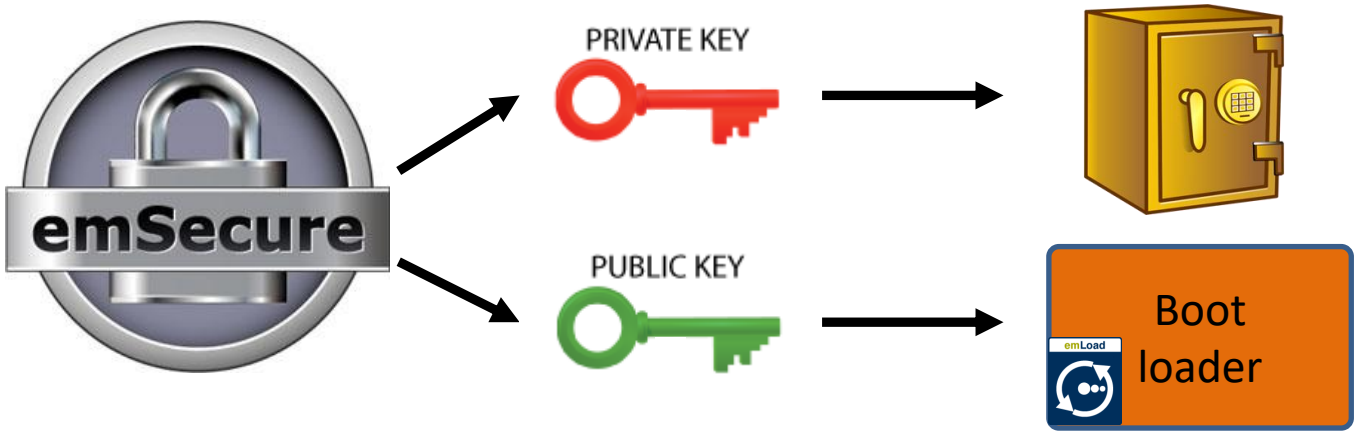
SSL, TLS 1.0, 1.1 and 1.2,
PKI X.509 certificates, crypto,
hashing and network protocols.



SSH and secure TCP/IP tunnel
embedded server and client,

Authorisation

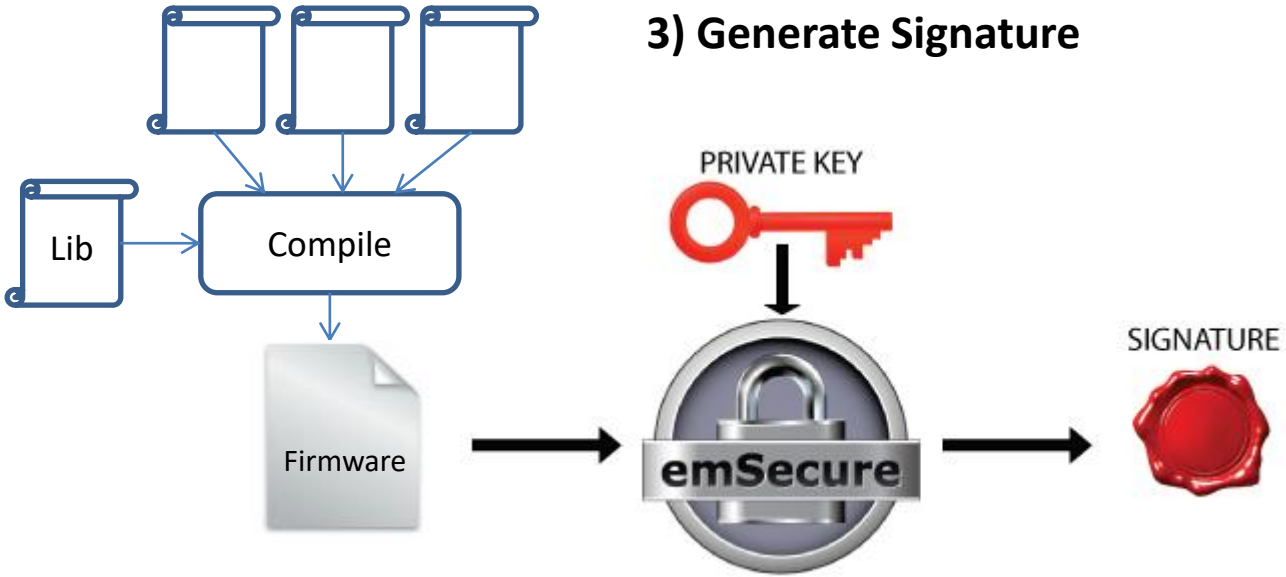
1) Create a key pair



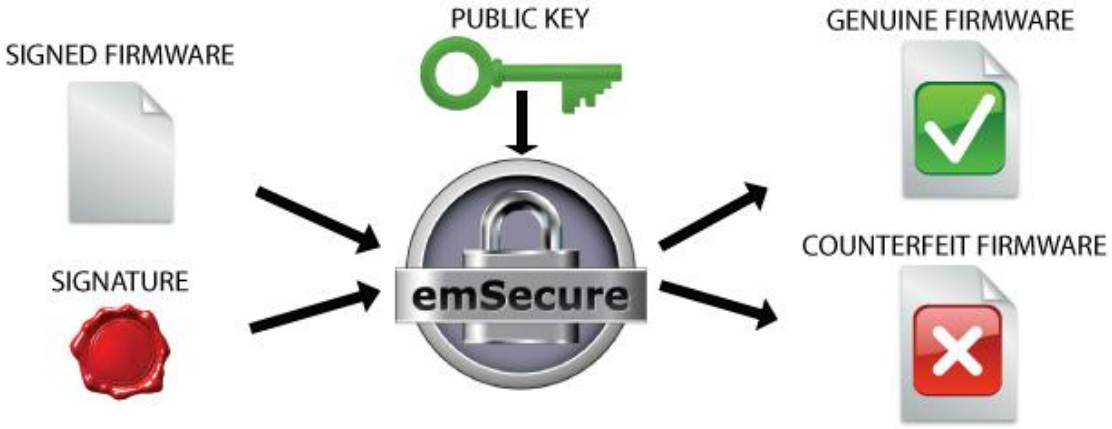
Authorisation

2) Generate application code

3) Generate Signature

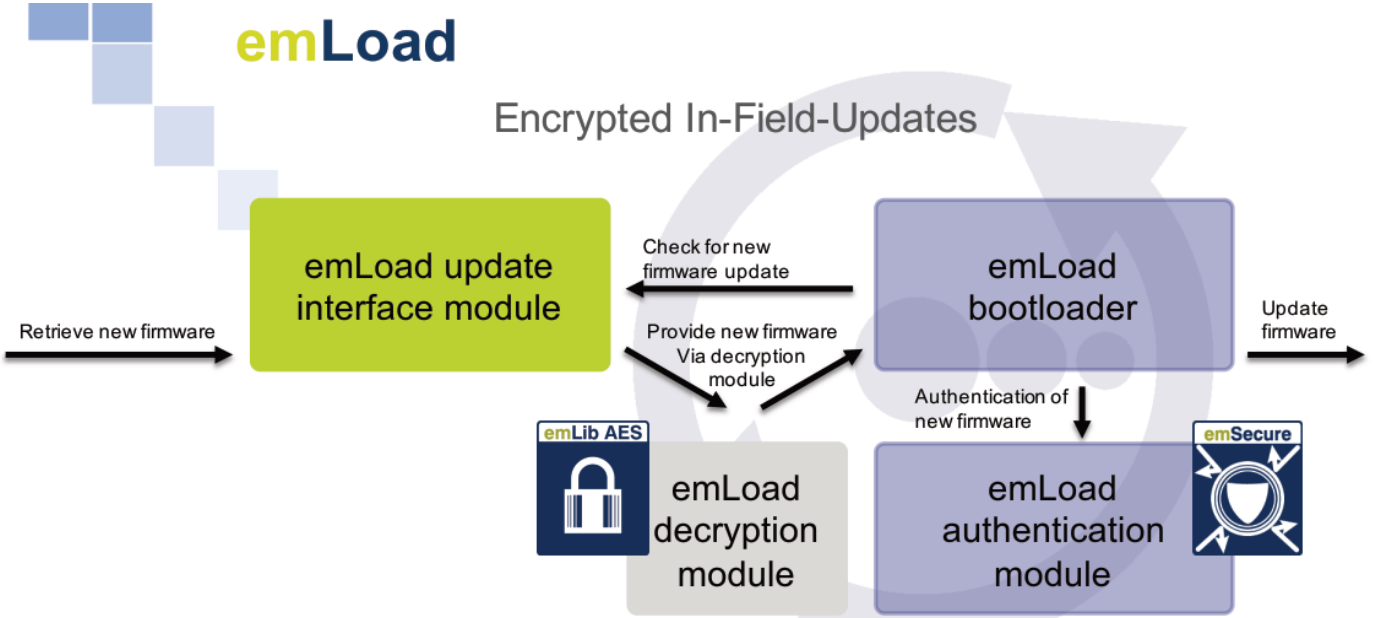


Secure bootloader



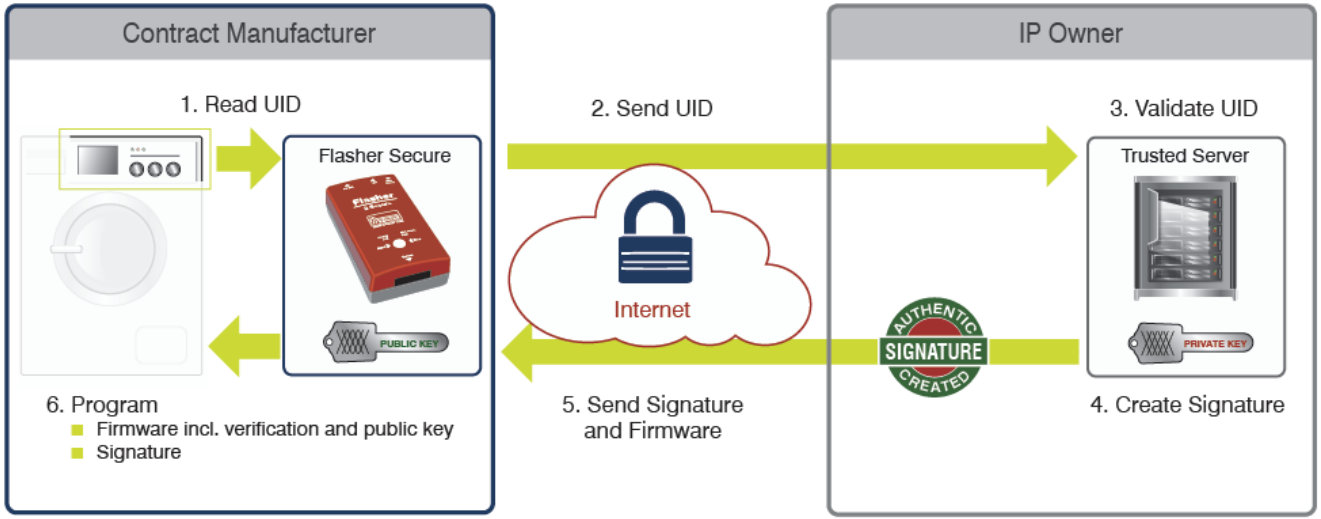
On a firmware update and when starting the product, the bootloader will verify the firmware by its signature. If they match, the firmware is started, otherwise the application will stay in the bootloader or even erase the firmware.

Secure bootloader



Or, take it one step further :

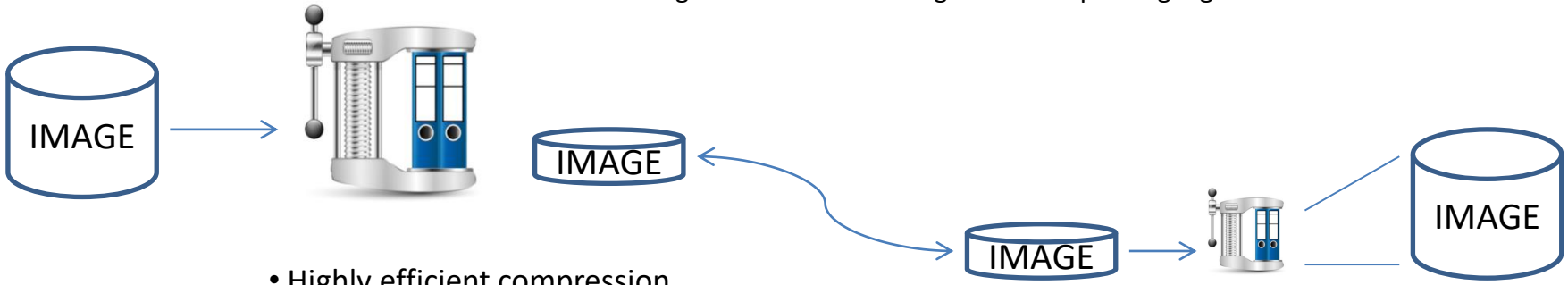
Or, take it one step further :



Low bandwith, small memory

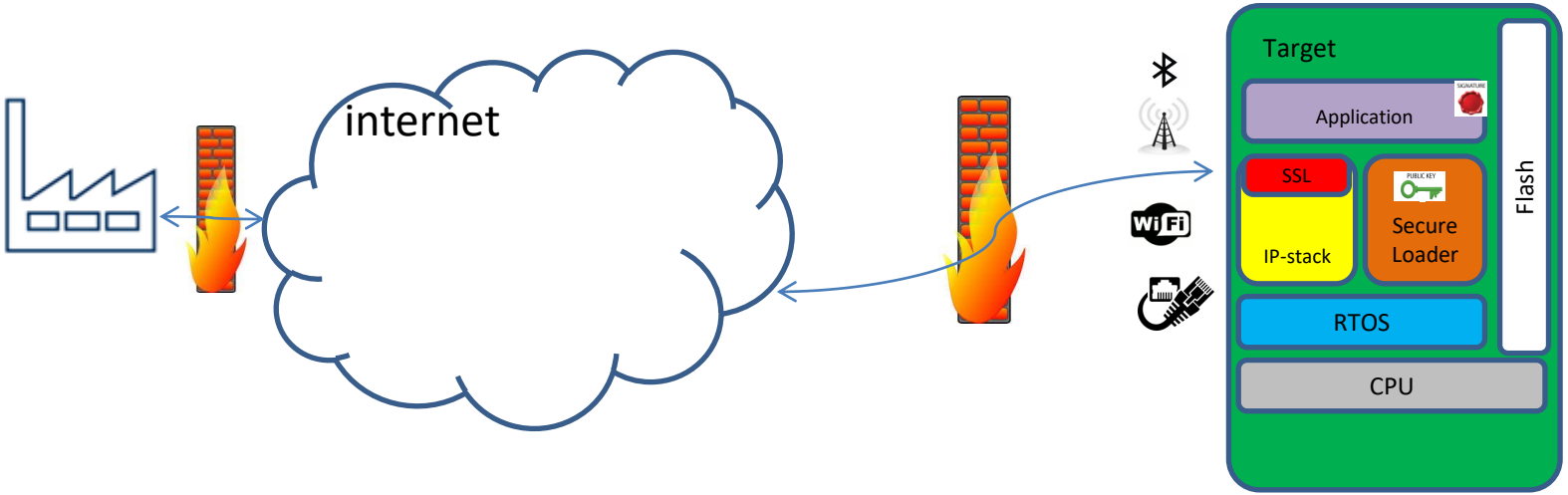
- Embedded “unzip”

Configuration bitstreams to program FPGA and CPLD devices.
Permanent files for embedded web server static content.
Upgrading firmware using a compressed image.
Storing user interface messages for multiple languages.

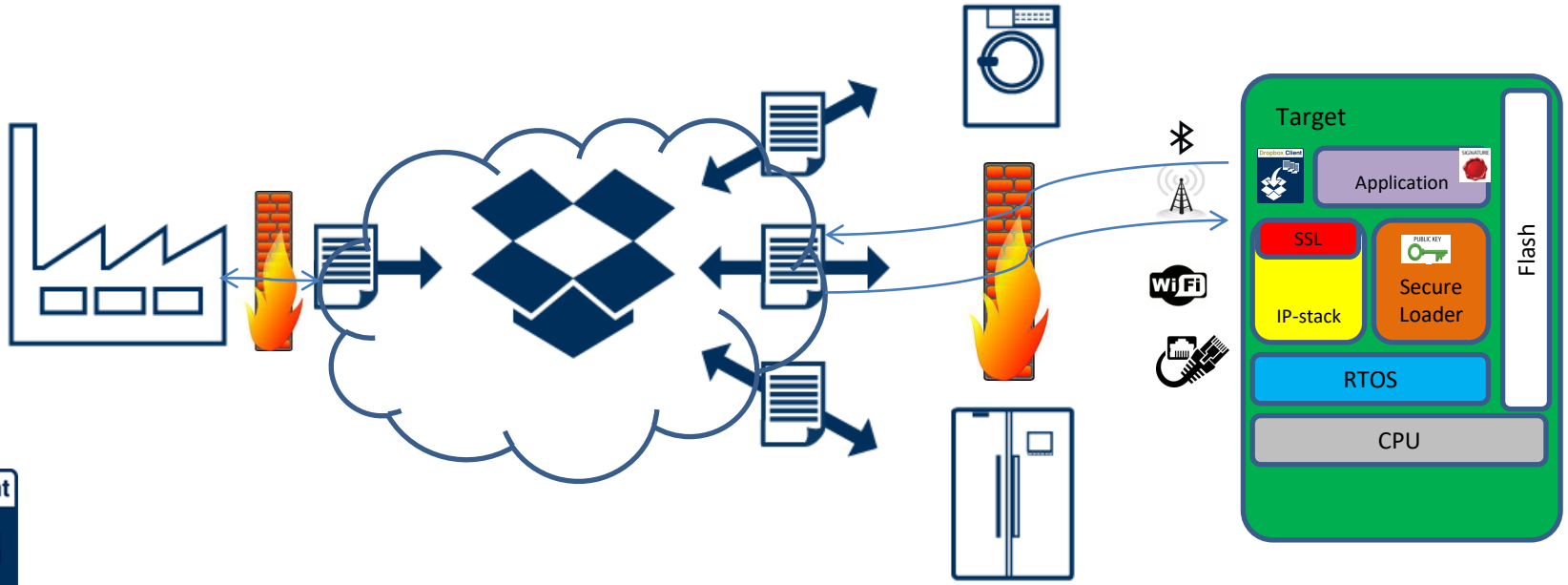


- Highly efficient compression
- (very) Small decompressor ROM footprint
- Fixed decompressor RAM use, chosen when compressing
- Wide range of codecs to choose from
- Automatic selection of best codec for each file

Transfer channel ..



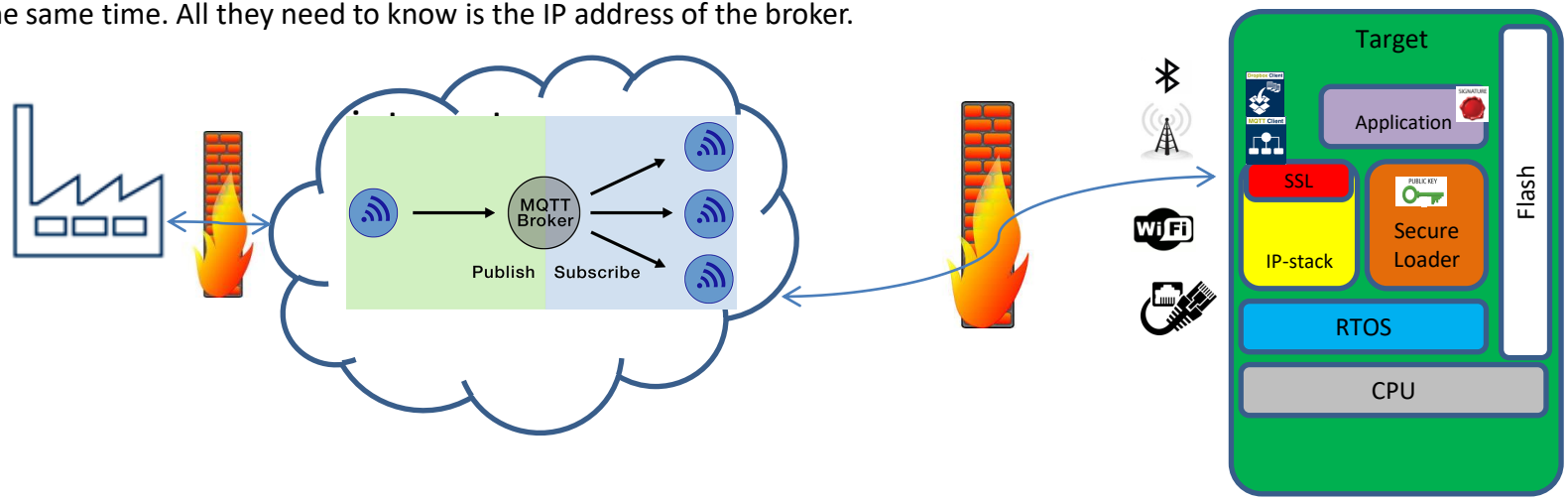
Transfer channel ..



Dropbox Client

Transfer channel ..

To get messages a from an MQTT broker a subscriber establishes a connection to the broker. The broker checks if a publisher has sent a message for the subscribed topic and if so, sends it to the subscriber. The advantage of this approach is that publisher and subscriber do not need to know each other and that they do not need to run at the same time. All they need to know is the IP address of the broker.



INDES-IDS BV - QuickStart service

- On-site assistance in setting up Tools, RTOS and middleware
- We can do the integration with your platform and application for you
- Local expert support
  - You give us (prototype) hardware so we can locally reproduce problems and support you
- Fixed price integration services

Seminar 20 juni :
Distributed Databases in networked embedded systems

- Relational Database
- Distributed, High Availability
- Fault tolerant, high reliability
- Replication, Synchronization, Data Recovery
- Secure (AES / SSL)

- Embedded, Android, iOS, Windows, Linux
- High performance, small footprint, scalable
- In-Memory, Flash, Disk, Hybrid

www.embedded-masterclass.nl

indes
The choice of professionals

For more information :

Stand 7D112

sales@indes.com

Tel : +31 (0)345 – 545.535

www.indes.com/embedded